PRMS®
the psychiatrists' program®

INTRODUCTION TO **ELECTRONIC HEALTH RECORDS**

INTRODUCTION

Many psychiatrists are making the decision to use electronic health records. For some, it's a continuation of the way they learned to practice in residency. For others, the decision is based upon a desire to enhance their practice with newer technology. And in some instances it's due to state laws mandating the use of EHRs.

The many benefits of electronic health records are evident: comprehensive and legible records, clinical decision support tools such as safety alerts, and remote access to records. These benefits should translate into improved quality of care and improved patient safety, which in turn should lead to decreased professional liability claims. However, history has shown that medical innovations are frequently accompanied by new risks and new areas of liability exposure, and so it is with electronic health records.

In this booklet, we take a look at the risks associated with use of EHR systems and offer suggestions for mitigating those risks. We also offer some suggestions for choosing a system and avoiding pitfalls when contracting with EHR vendors. It is neither our intent to encourage you nor to dissuade you from using electronic health records, but only to make you aware of possible risk issues so that you can make a decision that is best for you, your practice, and your patients.

GETTING STARTED: UNDERSTANDING TYPES OF SYSTEMS

With so many electronic health record systems out there, it's difficult to know where to begin – particularly if you are new to EHR use. A good first step is to understand the various types of systems. One way to approach the various EHR systems is to consider where the data resides - or more specifically, where the servers on which the data is stored are located.

Physician-hosted system: With this type of system, the EHR data is stored on the physician's own servers. In addition to purchasing the hardware (including servers) and software, the physician is responsible for maintenance, security, and data backup.

Remotely hosted system: Here the EHR data is stored on another entity's servers. The other entity is responsible for storing the data and also for maintenance, security and data backup. The data is under the control of the third party (the owner of the servers where the data are stored) rather than under the control of the physician. Generally speaking, there are the following three types of remotely hosted EHR systems:

- *Subsidized system:* With a subsidized system, an entity with whom the physician has a relationship (such as a hospital), subsidizes the financing for the EHR. Typically the subsidizing entity's servers are utilized rather than the physician's so the physician does not have control over the data. While cost-effective for the physician, potential problems include ownership of data (and access to it) if the physician ends his relationship with the entity as well as concerns regarding anti-trust or anti-kickback issues particularly if subsidized by a hospital.
- *Dedicated-hosted system:* Under this system, the physician does not store the EHR data on his own servers. Rather the data is stored on the vendor's dedicated servers. While the physician does not have control in terms of data storage, the data is stored on servers in specific, known physical locations.
- *Cloud-based system (internet-based computing):* With a cloud-based system, the EHR data is stored by the vendor on the internet (in the cloud). Such vendors are called "SaaS" (software as a service) providers. The physician's computers do not have the EHR software but rather the software is accessed through the vendor's website. Vendors tend to move the data frequently, so the physician

may not know where the data is located, other than "somewhere in the clouds." The physician does not have control of the data nor any control over when or to where it is moved. Because many cloud-based systems are offered free of charge or at lower rates than other systems, they are often chosen by solo practitioners and other small practices. Physicians must understand, however, that a free system isn't necessarily without cost. In addition to dealing with advertisements, those choosing a free system will likely have to contend with the fact that their personal data – and that of their patients – will be sold.

CHOOSING A SYSTEM

What Do You Need the System to Do?

In some ways, buying an EHR system is like buying a new car. It's easy to initially be swayed by all of the bells and whistles but ultimately you come up with a list of things that are must haves and so it is with an EHR system.

Think about how you practice. What are your basic needs to continue functioning as you do now? What additional capabilities would help you to practice more efficiently? For example:

- The ability to dictate notes
- E-prescribing capabilities
- Electronically generated claims
- Appointment scheduling
- Scanning capabilities
- Automatically generated thank you notes to referring physicians
- Remote access
- Ability to interface with other systems within your office
- Etc.

Those who are unfamiliar with electronic health records may not realize what features are actually possible in an EHR. An excellent resource for learning more about EHR system capabilities in general and evaluating particular systems is the APA's "EHR Requirements Document Tutorial" which may be found on their website www.psych.org.

Will This Particular System Function According to Your Needs?

Yes, it's slick. Yes, the display is visually appealing. But does it actually do what you need it to do the way you need it to do it? Will the system allow you to function in a way that seems natural or are you going to have to rethink how you do everything?

Of course one of the reasons you're contemplating an EHR system may be that you want to change the way you do certain things but be careful to avoid a system that so interferes with your workflow that it causes your focus to shift from patient care to correctly using the EHR system. Any system will likely take some getting used to. You and your staff may have to make some procedural changes and you can expect for there to be a learning curve and for tasks to initially take longer, but if the system forces you to completely change the way you document or perform other tasks, it may not be the right system for you.

Many psychiatrists have found this to be an issue when using certain cloud-based systems that have been developed for other specialties which often have vastly different methods of evaluating patients and documenting care. For this reason, you may wish to look for systems that were created specifically for mental health providers or have components that may be added that are psychiatry-specific.

Who Owns the Data?

If it's not stored on your servers, and you have no control over its movement, is it still your data? This is a question that you need to ask and have answered when contemplating any system other than a physician-hosted system. Be aware, however, that even with that type of system, a vendor may be able to include a disabling code in their software. This means that in the event of a dispute (such a as over price), the vendor can essentially hold your data hostage.

Your records are essential for quality patient care and are your primary means of demonstrating the practice of responsible medicine during the course of treatment. In the event of a claim or board action, your treatment record is your primary mode of defense. Accordingly, any gap in access to your records could result not only in harm to your patients but also could render a case indefensible.

What Tech Support Will Be Available?

Everything may seem simple and straightforward when you're speaking to a sales rep or being lead through the online tutorial, but it's often different when you're on your own

and dealing with real patient data. Remember that smart phone or that tablet that you bought that can do all of those amazing things if you could just remember how to do them? You don't want the same thing to happen with your EHR system.

Be sure and ask what kind of tech support you're going to have not only in the beginning but throughout the term of the contract. Are you a person who is comfortable with technology or are you going to need a bit more assistance? Will that be available? Will there be an extra cost? What about training new employees? Will there be support in the event of a system failure? Will it be available 24/7? (See also Tech Support on page 16)

Will the System Meet Evidentiary Requirements?

Many psychiatrists maintain progress notes by typing them first into Word and then printing them out, signing and dating the note, and then filing it into the patient's chart. This is a perfectly acceptable practice. What is problematic, however, is when the psychiatrist does not print the note but instead maintains it on his computer thinking that, as it is electronically accessible, it constitutes an electronic health record. It does not. And although it might be a useful method of record-keeping, those carefully kept notes may not be available to assist in the event of litigation as records kept in this manner likely would not be admissible in court.

What may come as a surprise is that even some systems that are actual electronic health records may not meet evidentiary requirements. The primary purpose of a medical record is of course to support patient care, but as stated previously, it is also key to establishing a physician's defense in the event of a claim or lawsuit. In order to be useful, however, the record must be able to be admitted as evidence in court. In their efforts to convert records from a paper system to an electronic system, some physicians have overlooked the question of whether their new system of record-keeping will allow them to generate a document that will be considered a legal health record and thus admissible. "Just because an EHR system creates something that looks like a medical record doesn't mean that document fits the legal definition of a medical record."[1]

Generally speaking, statements made outside of court by a party to a lawsuit are considered hearsay and are not admissible as evidence. The Federal Rules of Evidence define hearsay as a "statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." (Fed.R.Evid. 801(c).)

Documentation in a medical record – whether paper or electronic - is technically hearsay; however, there is an exception to the hearsay rule for records made in the regular course of business as are medical records. In order to qualify for this exception, records must be:

- Documented in the normal course of business
- Kept in the normal course of business
- Made at or near the time of the matter recorded
- Made by a person within the business with knowledge of the acts, events, conditions, opinions, or diagnoses appearing in it.[2]

The basic rules that allow a medical record to constitute a business record and thus be admissible in court are the same for both paper and electronic records.[3] "The key to the admissibility of business records at trial is that they are prepared and maintained in accordance with the Federal Rules of Evidence (803(6)). The person testifying or certifying the records for trial must be conversant with the policies and the processes used to ensure accuracy of the records."[4]

In order for an electronic health record to be admissible, the system upon which it is maintained must be proven to be accurate and trustworthy. Factors that may be used to determine this include:

- Type of computer used and its acceptance as standard and efficient equipment
- The record's method of operation
- The method and circumstances of preparing the record including:
  - The sources of the information on which it is based
  - The procedures for entering information into and retrieving information from the computer
  - The controls and checks used as well as the tests made to ensure accuracy and reliability of the record
  - The information has not been altered[5]

As such, the AMA suggests that there are three important things to consider when shopping for an EHR system that will allow for admissibility:

- How well does the system show authorship? Does it clearly show who entered what portion of the record?

- How does the system deal with changes? Does it track alterations to the record as well as who made each change and when? Does it save the original?
    - » How well does the system's audit function support the accuracy and validity of the record? Are there cross-checks in place?[2]
- In addition to querying your potential vendor on factors that support admissibility, it is also a good idea to consult your attorney, who can advise you on requirements specific to your jurisdiction.

Will Others Be Able to Utilize the Information When Not Using the System?

While it may be easy enough to find all of the necessary information that you need to provide care to the patient, will you be able to satisfy other needs? For example, if another physician needs medical information, can you easily provide him with the specific information he needs in a readable format? What about fulfilling record requests in litigation? If someone needs a copy of a portion of the record (or all of it) can you provide printed copies, as well as electronic copies?

CONTRACTING WITH EHR VENDORS

In selecting a system the vendor contract or user agreement is often overlooked. This is particularly true when the system is one that is obtained at very little or no cost. Let's face it. We've all done it. In our eagerness to access an internet program, we've readily agreed to terms we haven't read by checking the "agree" box and continuing on to the information we desire. Most of the time, this may be a low risk but that is not necessarily the case with an EHR contract. Two important facts: 1) these sorts of agreements are enforceable (regardless of whether they have been read) and 2) they often contain pages and pages of provisions that not only disclaim the vendor's obligations but also expose the physicians themselves to liability in the event of problems with the system.

You should not let this dissuade you from using electronic health records. But it is imperative that before doing so, you take steps to minimize your own exposure by reviewing – or better yet having an attorney review – the contract. EHR vendors want to do business with you but they also want to protect their own interests and their lawyers

have obliged them by drafting contracts in the most favorable terms possible.

Set forth below are provisions typically found in EHR vendor agreements along with sections that may not be in the agreement but need to be addressed. This list is by no means exhaustive but is intended to make you aware of the hidden dangers and hopefully to encourage you to seek legal counsel before entering into an agreement.

Definitions

If included, the definition section will typically be one of the first – if not the first – provisions in the agreement. The importance of the definition section is that it lends explanation to seemingly equivocal terms that may or may not carry the definition commonly associated with them. For example, "User." Does "user" mean an identified, particular person or does it mean a (class) of persons, e.g., physicians or mid-level providers? Or, does it mean anyone accessing the system at a particular time? Depending upon other sections of the document, for example the "license" section, this distinction may take on greater importance than one would typically expect. What about "access to data?" You would naturally assume that you would have the same access to your data as you do now but that may not be the case. Data access may be limited to certain time periods. Carefully read over the contract definitions, or if the agreement does not contain a specific section, note how terms are defined within other sections. If it is still not clear, ask for clarification in writing. (See "entire agreement" below.)

License

A license in this context means your right to use the vendor's software. You are not buying the actual software, only the right to use it. Once you are granted a license, you will want to know how long that license is good for. Is it ongoing for as long as you have the contract? A perpetual license is preferable to that of a fixed term. If it is for a fixed term, make certain that you know up front what the fees will be to renew the license. What about updates? Are updates included or will there be an additional cost? What is that cost? What about additional users? What if additional users are needed in the future – will they tell you what those additional fees will be now?

Fees

If you have opted for a fee-based system, you may notice that it is difficult to ascertain a bottom line price as there are typically a number of variables that affect the final cost. Many of these are discussed in other sections of this article. Make certain that you

understand the various fees and how and to what extent they may increase over time.

Another option is to go with a system that is available free of charge. Providers of free software utilize different business models in order to generate revenue. Some sell your de-identified data (your personal as well as that of your patients) to drug companies and researchers. While they may not come right out and tell you this in the vendor agreement, if they don't expressly state that they will not do it, you must assume that it is a possibility. Other vendors utilize advertisements within the EHR. You may have the option of viewing the system and may determine that advertisements won't be a problem for you. But remember, things can change. The vendor can decide to increase the number of advertisements which may move you to opt for an ad-free system at a fee. Even if you are going with the free system now, take the time to learn what the service fees are for an ad-free system and learn whether those are subject to change, how often, and how much. You do not want to find yourself hooked into a system that becomes cumbersome to use and then have to pay unanticipated fees to convert to a usable system. Bear in mind also that certain features such as tech support, 24/7 access to records, and additional storage space may not be free and may in fact be quite expensive.

Contained within these provisions, will also be a discussion of payment – when and how it is to be made. Recognize that the penalties for late payment (even by as much as a few days) may entitle the vendor to block your access to your medical records. In this instance, they may also charge a hefty reconnection fee as well as late charges and interest.

Warranties

As defined by Black's Law Dictionary, a warranty is "an assurance or guaranty, either express if in the form of a statement by a seller of goods, or implied by law, having reference to and ensuring the character, quality, or fitness of purpose of the goods."

When you purchase or subscribe to an EHR service you undoubtedly have certain expectations – for example you expect that the system will perform as advertised, that it will generate accurate information, that it will not lose your data, that it will protect your data from security breaches, just to name a few. You would probably be quite surprised to learn then that the vendor may have provisions in the contract whereby it specifically states that none of these things are warrantied unless they are expressly stated in the contract.

Commercial transactions are governed by the Uniform Commercial Code (UCC) which is a set of uniform laws that has been adopted in whole or substantial part by all states.

While it is clear that the UCC applies to the sale of goods (such as a computer system) there is a question as to whether the UCC actually applies to the provision software or software as a service (SaaS) which is what cloud-based EHR systems are. Despite this, in drafting their contracts, most EHR vendors will follow the UCC rule that "the exclusion or modification of implied warranties of merchantability must be conspicuous." (UCC § 2-316(2).) That is why half of your contract may be written in capital letters. It is in these sections that the vendor will attempt to limit or deny most if not all implied warranties.

Entire Agreement

An important provision that is typically relegated to the back of the agreement – usually mixed in with all of the language that appears just to be the superfluous stuff that is at the end of most contracts – will be a provision labeled "entire agreement." It will state something to the effect that the document (and other documents attached or hyperlinked) represents the entire agreement between the parties. In other words, if you don't see it there, it cannot be enforced. That verbal promise the vendor made and confirmed in an email? If it's not in the final agreement, it is not enforceable. What this means is that if there is a provision in the contract that you are unhappy with that the vendor agrees to amend, or if the vendor provides a clarification for a cryptic provision, the contract needs to reflect those changes or explanations for them to be enforceable.

As a side note, if you do (and we really hope you do) have an attorney review your contract, remember that he or she will likely not have been privy to your discussions with your vendor representative and thus it may be difficult to ascertain whether the written contract does in fact reflect the entire agreement as you yourself understood it to be. To aid your attorney in this process, keep notes of what was discussed and or promised.

Choice of Law

Choice of law refers to what state's laws will govern the contract in the event of a dispute. You're probably thinking, "This doesn't sound like a big deal. We're all in the U.S., how different can the laws be?" And you're right, this isn't a huge issue *until* there is a dispute. That's when you realize that you're sitting in Virginia and the contract in question is governed by the laws of another state several hundred miles away. This then forces you to try to find an attorney in the other state and possibly even travel there yourself. Ideally, the contract will state that the contract will be governed by the laws of your own state.

Confidentiality, Privacy, Security

While one would understandably think this section sets forth the vendor's obligation to maintain the confidentiality, privacy, and security of your patient records, in fact, this section often deals primary with *your* obligations with regard to the *vendor's* information. Here you typically agree not to disclose any of the vendor's intellectual property, copy software, etc. Some may even go so far as to include a gag clause – a clause prohibiting you from disclosing to others problems with the EHR system.

Breach

A breach is a failure to perform under the terms of the contract. A breach may be material, i.e., so significant that it excuses the other party from their obligations, or it may be partial. A breach may occur as a result of one party's failure to do something it had contracted to do (for example, provide a service) or as a result of the party's performing an act it agreed not to do (for example, disclose confidential information).

In some instances, a contract will clearly set forth what constitutes a breach of the agreement. In others, one has to glean what constitutes a breach - often by reading through many pages of obscure language. Most EHR contracts will clearly elucidate what activities you must and may not perform; however, it may be quite difficult to ascertain what activities on the part of the vendor may be deemed to be a breach of the agreement. If you look closely at the disclaimers in the warranties section, you will likely note that the vendor typically doesn't claim that their product is fit for any particular purpose or that you can rely upon it in any way. Your data might be lost or disclosed inappropriately and still, this is not a breach of the agreement because they never promised this wouldn't happen.

If one party is deemed by the other to be in breach of the agreement, there is typically a procedure by which the aggrieved party must notify the other of their failure to perform under the terms of the contract. Unless it is a material breach which justifies immediate termination, the offending party will have a period of time in which to cure its breach. Make certain that there is no provision in the contract that allows the vendor to deny you access to your records in the event of a breach on your part.

Termination

The termination section of your contract is possibly the single most important thing to know about and also a section many give little thought to. Your contract may specify a contract term, how it may be renewed, and how notice of termination must be given. At

first glance, that might appear sufficient, but is it? You know that you can get out of the agreement, but what about your data? What happens to it? Will you get it back? In a usable form? Without paying additional fees? Will the vendor keep a copy?

Terminating an EHR contract can be something akin to a divorce where there is a custody battle only rather than fighting over children, the dispute is about your patient records. This was a hard lesson learned by Milwaukee Health Services (MHS) in the summer of 2013. MHS decided to end its long relationship with Business Computer Applications (BCA) at the end of the contract period per the terms of their agreement. What the agreement apparently did not address was the disposition of the medical records. At the end of the contract term, BCA refused to give MHS access to their data saying that MHS owed them for past due amounts and required an additional sum to convert the data to a usable format. MHS tried to file an injunction against the retention of their information but the court was not sympathetic. It stated that MHS had literally years to resolve the issue of what would become of data after the contract was terminated and failed to plan appropriately.

Inability to access patient information not only subjects you to liability exposure if errors are made but also exposes you to the possibility of a licensure action for failing to maintain medical records per the laws of your state. Thus in addition to a clear understanding of how a contract may be terminated, you will ideally also have what amounts to a "prenuptial" agreement in place to deal with what happens to your records when the relationship ends. One suggestion is that you look for a disentanglement clause – a provision that requires the vendor to use reasonable efforts to assist you in migrating your data to another vendor.

Make certain also that you know what happens to your data in the event the vendor goes broke or has to shut down. Yes, you've chosen a reputable company and it seems highly unlikely today that this would happen, but can you say "Gateway computer?"

Limitation of Liability

Because the vendor has likely excluded all warranties, it will have substantially already limited its liability exposure. But just to be on the safe side, in this section the vendor will make certain that it has further exculpated itself from any possible liability. Just to be certain that all bases are covered, the vendor may add in a provision limiting your allowable damages. For example, on free cloud-based system vendor limits their liability to the actual fees paid by the user in the previous six months. As it's a free system and the user pays nothing, that means he is entitled to absolutely nothing – no matter what.

Hold Harmless and Indemnification Clauses

Many psychiatrists are familiar with hold harmless and indemnification provisions having seen them in contracts with third-party payers or in certain employment agreements. For those who are not familiar with them, indemnification clauses transfer liability from one party (in this case, the vendor) to the other (the physician) essentially requiring them to cover their losses as the result of third party claims – even if the cause of loss was the vendor's faulty system. In addition, they may preclude one party (again typically the physician) from seeking damages against the other party.

To illustrate how an indemnification agreement might come into play, consider the following scenario. A patient receives inappropriate care during a hospitalization. In an effort to explain the error, the hospital indicates that the harm to the patient is due to a problem with the EHR system. In any resulting litigation, by placing blame on the EHR system, the hospital may also have caused the EHR vender to be sued. If an indemnification agreement is in place, any monies owed by the vendor as a result of a verdict or settlement, and any associated attorney's fees, would be the responsibility of the hospital. And while the hospital is undoubtedly well-insured for its own liability, it is unlikely that that insurance would cover the liability of the EHR vendor.

Amendments to the Agreement

As stated previously, the contract itself contains the entire agreement between the parties but there is often another provision that states that the agreement can be amended. Familiarize yourself with this section to determine whether you are allowed to ask for modifications once the contract takes effect and whether you can terminate the agreement if your requested modifications are not made. While there may not be an opportunity for you to make contract modifications, there will undoubtedly be a provision in the contract stating that the vendor retains the right to make modifications to the agreement from time to time. Know how this will be done, i.e., what type of notice you will receive. Will it be sent to you or will they simply update the contract from time to time requiring you to reread it on regular basis? If you don't object with in a specific amount of time, it is usually stated that you by default will have agreed to the terms.

ADDITIONAL TOPICS TO BE ADDRESSED

Training

It happens to the best of us. We buy the new computer or phone or download the app that can do so many wonderful things – or at least it would if we could figure out/had the time to learn how to use it. Yes, there are instructions but that can be time-consuming and frankly tedious.

And the instructions may not be clear. In order to get the most out of your system, in all likelihood you will need some type of training. Perhaps it's a tutorial or perhaps someone will come to your office. Will a user manual be provided? Whichever way, you want to make sure that it's spelled out in the contract. Otherwise, it's not necessarily part of the deal. And what about later? If you hire another provider, will training be available to him/her or will you just have to pass on what you've learned? Is training of additional individuals included in the initial price or will there be an additional cost? Do you know what that cost is now or is it a sum that will be determined at a later date? What about system upgrades? Will training be required?

Tech Support

The system was working fine yesterday but now suddenly the system keeps freezing up or the cloud went down and you can't gain access. What in the heck are you supposed to do? Does the vendor have someone who can assist you? Is this person only available during normal business hours or 24/7? Is there an extra fee for this? How much is it? Is it by the hour? Does it matter whether the problem stems from something you may have done or something that occurred on the vendor's end? Will it be available as long as you have the system or only for an initial period? Can you extend availability by paying an additional fee? If so, how much? Who provides tech support? If it is outsourced to another country, there may be a language barrier that makes communication difficult. Do you know how to access tech support? Can they be reached by phone? Email? Live chat? How quickly can you expect a response from the vendor? What if the vendor uses a subcontractor for data storage and you're having access issues? Does the contract state that it is the vendor who is responsible for ensuring uptime and access to data or must you deal with the subcontractor?

Disaster Recovery

How is data backed up? How often? Where is the backup server located in relation to the

main server? Does the possibility exist that the same disaster could impact both? What is the vendor promising with regard to disaster recovery? Sadly, if you read the contract closely, you may find that the vendor has declared that it is not responsible for any loss of data.

HIPAA

Without going too far afield, it probably makes sense to spend a moment here on the topic of HIPAA. Under HIPAA, if you are a covered entity, you must ensure that there is a Business Associate Agreement in place with the EHR vendor who will have access to your patient information. Under this agreement, the vendor agrees to maintain the confidentiality, security, and integrity of your patients' records. Also included are provisions requiring notification to you in the event of a breach involving your patients' information.

While all psychiatrists are required to maintain the confidentiality of patient information, not all psychiatrists are actually covered entities. If you are not technically a covered entity under HIPAA, you need your EHR vendor's written agreement to protect your patient information, and it can be in the form of a Business Associate Agreement.

Much of what is contained in a business associate agreement is language that is required under the HIPAA regulations. Sometimes, vendors will make a business associate agreement a separate document that contains purely the material required by regulation. Other times they will use the business associate agreement as a vehicle in which to hide other provisions that are absolutely NOT required under federal law such as indemnification provisions.

RISK MANAGEMENT REMINDERS

- "Click and agree" online agreements may not be negotiable and are legally binding
- Consider consulting an attorney before signing a vendor agreement
- A system billed as "free" may in fact have hidden costs
- Know what will happen to your data in the event of the vendor's insolvency or termination of your agreement
- Watch out for indemnification agreements
- Ensure that all issues are resolved with the vendor before signing the agreement
- Understand state law and HIPAA requirements regarding EHR systems
- Have a Business Associate Agreement or similar confidentiality agreement with the vendor

Obviously vendors will have greater impetus to negotiate if you are actually paying for the system and may be unwilling to make any changes to a free system. In that case, you need to make certain that you are comfortable with the contract "as is" and are ready to assume the risks it presents. You may then decide that even if there is cost involved, a paid vendor's willingness to negotiate the contract may make it worth that cost.

OPERATING AN EHR SYSTEM

Transitioning from Paper to Electronic Records

Unless you are starting your practice from day one using an EHR system, you are going to have a period of transition. It is during this time that you must be particularly vigilant to avoid documentation errors and gaps. Courts and licensing boards will not "cut you any slack" during your transition/learning period. You will be expected to practice to the same standard of care and are responsible for implementing procedures a reasonable provider would implement to avoid errors. To that end, you should recognize, and take steps to minimize, the following risks:

- Documentation gaps – how will you maintain and refer to your paper charts?
- Mental fatigue from treating patients while learning a new system
- Inadequate training/inconsistent use among staff leading to errors

Documentation & EHRs

Now that you are ready to implement your new system, you must now think about the risks associated with EHR use and take steps to mitigate those risks. The first thing to remember is that no matter how good the system, what you get out of it will only be as good as what you put in. In other words, garbage in, garbage out. If you have not been thorough with your documentation in the past, your EHR system might make your record look "prettier" but it will not in and of itself create a record that supports good patient care and would be useful in your defense in the event of a claim or a lawsuit.

Because most of the risks associated with EHR use have to due with documentation, it probably makes sense then to briefly go over the basics to make certain that you are including everything that should be in a patient's record. Your medical record has

three essential purposes/uses: to support good clinical care, to use in your defense and show compliance with legal requirements, and to substantiate your billing and demonstrate your adherence to payer guidelines. To that end, your records should:

- Be timely
- Include a date for every entry
- Include the patient's name on every page
- Include standard abbreviations
- Be documented discretely
- Clearly show corrections/changes
- Provide contemporaneous assessment of your patient's needs and behaviors
- Substantiate your clinical judgment and choices
- Document explanations of your treatment decisions, significant events, and revisions to the treatment plan
- Demonstrate informed consent
- Include telephone calls (and other communication such as email) with and about patients
- Document prescriptions and refills
- Document missed appointments

In order to produce a legally sound health record, the American Health Information Management Association (AHIMA) further recommends that:

- Specific, rather than vague or generalized, language be used. Avoid phrases such as "patient is doing well" or "status quo." Physicians should not speculate and should report factual information. If a diagnosis is not yet known, documentation should clearly identify speculation versus factual information.
- Chart objective facts – what can be seen, heard, touched, and smelled. Use quotations when quoting the patient and document the patient's response to care.
- Document complete facts and pertinent information.[2]

DOCUMENTATION RISKS ASSOCIATED WITH EHRs

Concerns about patient safety and the use of electronic health records have been in the news for years. As the use of this technology has grown so have these concerns. In 2015 ECRI Institute listed errors associated with EHR use among its Top 10 Patient Safety Concerns and the Joint Commission issued a Sentinel Event Alert on the Safe Use of Health Information Technology.

Documentation Shortcuts

Documentation shortcuts were created with the intent of allowing physicians to create a more complete record in less time. Ironically, it is often these shortcuts that pose the greatest risks to patient safety and physician liability.

Box Checking

A written record often contains seemingly extraneous information that can become extremely important to a physician's defense. For example, who was present when a patient was informed of the risks associated with a certain medication and what questions were asked and answered, or what comments the patient made regarding her adherence to treatment. Unfortunately, some EHR systems don't provide a mechanism for users to include this information and instead they are limited to checking boxes. The absence of the ability to write a complete narrative is a frustration many physicians report with EHR use.

Templates

As will be discussed more fully in a moment, template use is an area that is undergoing scrutiny by CMS and other payers. Templates are used to easily provide additional detail to a note but may not accurately reflect treatment – for example, they may misstate a patient's age or gender. The result is often a record filled with a large number of identical notes which call into question whether the physician truly did a thorough evaluation of the patient at each encounter. If a template is used for informed consent, it may not capture all of the information you need to establish that the informed consent discussion actually took place, e.g., who was present.

Autopopulation

Some systems will automatically populate entries with information from previous visits. On occasion the system will erroneously enter information from the previous patient. It is often impossible to determine whether data was entered by a clinician or by the system itself.

Relying on default data can cause you to make false assumptions about a patient's condition and making inaccurate default data a part of your record will cause you to lose credibility in any subsequent litigation. Further, some state medical boards have written position statements cautioning licensees against relying upon software that pre-populates fields.

Copy and Paste Functionality or Note Cloning

As with template use, this function which allows a provider to copy and paste portions of previous entries into a new note is undergoing scrutiny by CMS. While intended to improve the thoroughness and ease of documentation, this function may be misused leading to problems both for the physician and the patient. Risks include:

- The possible perpetuation of erroneous information leading to incorrect diagnosis/treatment
- The potential for copying and pasting the note to the wrong treatment date or even the wrong patient's record
- The inability to identify the author of the original note and the date of that note
- Duplication of information not relevant to the current encounter

In its *Report of the Committee on Ethics and Professionalism in the Adoption and Use of Electronic Health Records,* the Federation of State Medical Boards recommends:

> "If a provider is satisfied that copying and pasting information into a new record entry is permissible in a given instance, he or she must include the appropriate citation in the record and verify that the copied information is current. Generally, it is inappropriate to copy and paste or otherwise document an entry that is not derived from a patient encounter at the time of the visit, unless the provider makes a clear notation that the information is copied and pasted from another record. Copy and paste is only appropriate when the content is verified."[6]

The False Claims Act (FCA)

The Federal False Claims Act (FCA) protects the federal government from being overcharged or sold substandard goods or services and imposes civil liability on anyone who knowingly submits, or causes to be submitted, a false or fraudulent claim. "Knowingly submits" includes acting in deliberate ignorance or reckless disregard of the truth or falsity of the information related to the claim. Penalties for violation of the FCA include fines up to three times the amount of damages sustained by the government plus $11,000 per claim filed, or jail, or both.

One example of "knowingly submitting" a false claim might be a situation involving "upcoding" where a provider bills for a higher code than is appropriate for the service actually furnished which then results in a higher payment. The use of templates or note cloning in an electronic health record may lead to upcoding which puts the physician at risk – even if the upcoding was unintentional. In September of 2012, HHS and the Justice Department sent a letter to the American Hospital Association and others advising that the use of templates and note cloning would thereafter be under scrutiny.

If you choose to use documentation shortcuts such as templates and the copy/paste function you must remember that it is you who will be responsible for insuring that the encounter is billed using the appropriate code. Though the system may create documentation that meets the coding requirements for the highest code, it does not mean that you should bill at that code. Medical necessity is the key to accurate coding – even if a coding tool suggests a higher level of service.

Too Much Information

Another issue to consider is whether so much information is being captured and stored that users cannot find relevant information. This can be problematic in emergency situations as well as routine treatment. One practical solution to this dilemma is to periodically print out a patient record and evaluate it for adequacy. A good medical record is one in which a subsequent provider or an expert witness would be able to understand what happened during the treatment relationship and why.

Metadata

Metadata is literally data about data and provides an audit trail of everything that occurs within the electronic record. What this means is that every time you sign onto an electronic health record system, you leave a trail of your activity including what patient records and what portions of those records were viewed, the actual time the record

was viewed, how much time was spent looking at the record (including how long it took to view and override a safety alert or other clinical support tool), what entries were made, and any changes that were made to the record. And, as with all other parts of the medical record, metadata may be discoverable in a medical malpractice lawsuit.

"In addition to affecting the risk of a lawsuit, implementation of EHRs may affect the course of malpractice litigation by increasing the availability of documentation with which to defend or prove a malpractice claim."[7] No longer will juries have to rely upon a physician's recollection as to what occurred. There will be no question as to whether a physician reviewed a lab finding or whether he or she made a self-serving entry after an adverse outcome. Any dispute may now be resolved by simply examining the metadata.

In addition to its use in malpractice litigation, metadata may also be utilized to monitor access to patient records and to uncover HIPAA violations. Another potential use is by third-party payers who wish to analyze it to determine whether physicians have actually performed the services for which the payers are being billed.

Clinical Decision Support Systems

Clinical decisions support systems are designed to assist physicians by making recommendations about possible diagnoses from a set of signs and symptoms, provide alerts on possible drug interactions or critical lab values, or to question a physician's medication dosage or other orders.[8] Unfortunately these systems tend to produce alerts that are not relevant and in such a large number that they've prompted at least one author to refer to them as the electronic version of the little boy who cried wolf. In other instances, the alerts may be based on out-of-date information. In fact, your EHR vendor likely will not even stand behind them as many include in the limitation of warranties section of their vendor agreements a statement that they are not responsible for the accuracy or completeness of the alert.

A 2009 study published in the Archives of Internal medicine found that of more than 200,000 alerts generated by an outpatient electronic prescription system, physicians accepted only 9.2% of drug interaction safety alerts and only 10.4% of "high severity interaction alerts."[9] Further, a Department of Veteran's Affairs funded study published in the April 2012 Issue of the International Journal of Medical informatics found that often prescribers were unsure of why the alert was generated or that it pertained to a group of individuals, e.g., diabetics or pregnant women, as opposed to the specific patient in question.[10]

Alerts are often seen as such a waste of time that some practices have elected to have that feature turned off if possible while others have purchased software that allows them to screen alerts for relevance. While it is true that many alerts are not clinically relevant it is also true that there are some that are and therein lies the problem. Physicians can become so accustomed to seeing alerts that are not relevant that they tend to not notice when an alert is relevant which is known as alert fatigue.

Unfortunately, a jury will not be sympathetic should you miss an alert that might have prevented patient harm. As presented by a plaintiff attorney, they will only see that you were told of potential patient harm and ignored the warning. Because the plaintiff attorney will also have access to metadata, he will be able to show how rapidly you clicked past the warning seemingly without consideration.

RISK MANAGEMENT REMINDERS

- Ensure templates used are appropriate for the specific patient
- Consider disabling the cut and paste function or use with extreme discretion and require author identification for each entry
- Do not allow autopopulation
- Periodically print out a copy of your record to look for:
  - Technical glitches
  - Ability to pass a billing audit
  - Ability of a subsequent treater (or an expert witness) to understand what you did and why
- Understand metadata
- Ensure appropriate security protections on hardware and software
- Ensure compliance with federal and state confidentiality law
- Prevent inappropriate access by employees – training is key

EHRs AND THEIR IMPACT UPON PATIENTS

There is a common fallacy that a psychiatrist must obtain a patient's permission before using an electronic health record; he does not. How you choose to document is strictly up to you. You may, however, want to consider what – if any – impact EHR use might have on your patients.

Problem: The Elephant in the Room

While some psychiatrists are continuing the practice of making brief hand-written notes during the session and then later writing a more expansive note which then goes into the system, others have begun bringing a laptop or tablet into the session itself. While most patients realize that much of their medical information is computerized, actually discussing a mental health issue and seeing that information entered into the system may cause anxiety for some. This, in turn, can result in patients being less than candid about symptoms for fear their privacy may be breached.

Solution:

Consider "introducing" patients to your computer and telling them how information is used within the practice. You should also wish to briefly discuss security, e.g., that only authorized users can view medical information, etc.

Problem: Talking and Typing is a Lot Tougher Than Talking and Taking Notes

Especially when the system is first introduced into your practice, you may find that there is a bit of a learning curve. While this is certainly understandable, you should be aware that your difficulty with the system may lead some patients to have concerns regarding the accuracy of your documentation.

Solution:

Part of this will be resolved with time as you become more familiar with your new system. In the meantime, acknowledge your difficulty. Many patients will be able to relate and most will appreciate knowing that even someone with the intellect of a physician faces the same challenges they do. You might also consider not bringing your laptop/tablet into the session until you've reached a reasonable level of proficiency.

Problem: The Patient Perceives That Your Attention is Focused on the Computer Rather Than on the Patient

It is a given that in order to find necessary information and to accurately input new information, a certain amount of focus will need to be on the computer screen. Although jotting down a note in a paper chart is easy enough to do while conversing with a patient, typing a note into an EHR may require more concentration.

Solution:

Maintain communication by engaging the patient verbally, visually, and/or posturally: continuing to speak to the patient while looking at the screen, periodically looking up and making eye contact especially while the patient is speaking, and positioning yourself in such a way as to turn toward the patient while focusing on the screen. Depending on screen placement, the last method may take some maneuvering, but it will suggest to the patient that you want to and are trying to focus your attention on the patient. You might also consider turning the screen so that patients can see information and encouraging them to actively participate by viewing parts of the record together.

Problem: Data Overload

With so much patient information right at your fingertips, they may be lulled into believing that you have everything you need and may be less inclined to ask the probing questions that were once a part of your session.

Solution:

Make a habit of reviewing and confirming information with the patient such as the problem and medication lists. Not only will this ensure that you have an accurate understanding of the patient's current medical situation, but it will further help the patient to feel that he or she, rather than the computer, is the focus of attention, helping to alleviate any discomfort the patient may have with its use.

By being cognizant of potential patient concerns with the use of computers within the exam room, you can take steps to ensure that EHRs continue to be the tools they were intended to be, rather than a hindrance to physician-patient communication.

CONCLUSION

Electronic health records as with any other tool used in medicine, have both the ability to enhance patient care and to jeopardize it. Physicians considering their use must engage in thoughtful selection, preparation, and training to ensure the safety of their patients and to protect their own liability exposure.

1. Dolan, PL. Is Your EMR legal? A Document Can Look Like a Medical Record, but Not Meet the Legal Definition, AMedNews, October 13, 2008.
2. AHIMA. Update: Maintaining a Legally Sound Health Record – Paper and Electronic. Journal of AHIMA 76 no. 10 (2005):64A-L.
3. Quinsey, CA. Foundational Concepts of the Legal EHR, Journal of AHIMA 78 no. 1 (2007):56-57.
4. AHIMA. The Legal Process and Electronic Health Records. Journal of AHIMA 76 no. 9 (2005): 96A-96D.
5. Journal of AHIMA 76 no. 10 (2005):64A-L.
6. Federation of State Medical Boards. Report of the Committee on Ethics and Professionalism In the Adoption and Use of Electronic Health Records, April 2014.
7. Mangalmurti SS, Murtagh L, Mello MM. Medical malpractice liability in the age of electronic health records. N Engl J Med 2010 Nov 18; 363(21): 2060-7.
8. Berner, ES. Ethical and Legal Issues in the Use of Clinical Decision Support Systems, J.Healthc Inf Manag. 2002 Fall; 16(4):34-7
9. Arch Intern Med. 2009;169(3): 305-311
10. Russ, AL, et al. Prescribers' interactions with medication alerts at the point of prescribing: A multi-method in situ investigation of the human-computer interaction. International Journal of Medical Informatics, Volume 81, Issue 4. 232-243.

PRMS

CONTACT US

(800) 245-3333
TheProgram@prms.com
PsychProgram.com

MORE THAN AN **INSURANCE POLICY**